SCADA Field Device Protection Profile Project

Target of Evaluation (TOE)

Introduction

The Process Control Security Requirements Forum (PCSRF) has a project to develop and complete a SCADA Field Device Protection Profile by April 30, 2006. The Protection Profile will list the security requirements for field devices such as PLC's, PAC's, RTU's and IED's.

The Protection Profile is an opportunity for the asset owners, vendors, industry organizations, government organizations and other interested parties to provide a clear and comprehensive set of security requirements for the next generation of field devices. Vendors will then be able to develop field devices that meet the Protection Profile requirements and have those devices independently tested and certified by an internationally recognized third party.

PCSRF has chosen to use the Common Criteria methodology to specify functional and assurance requirements. The Common Criteria has a precise language and methodology that enables for clear specifications and objective testing. To achieve this, the Common Criteria sacrifices readability and is not the appropriate document for a general reader to learn guidelines or best practices. It may not be easy for even a subject matter expert in SCADA Field Devices to understand some of the later sections of the Protection Profile text.

To encourage participation each milestone deliverable in this project will have a section with the draft Protection Profile text and a section explaining the Protection Profile text.

We need your comments on either the Protection Profile text or the explanatory text. If you can identify an issue in the explanatory text, we can convert it into the proper Common Criteria format.

There are helpful books available, such as Debra Herrmann's *Using the Common Criteria for IT Security Evaluations*, if you want to understand the specific Common Criteria language. As Ms. Herrman defines it, the Common Criteria "provide a complete methodology, notation, and syntax for specifying requirements, designing a security architecture, and verifying the security integrity of an 'as built' product, system or network."

PLEASE SUBMIT COMMENTS FOR MILESTONE 1 BY OCTOBER 24, 2005

SUBMIT COMMENTS TO: peterson@digitalbond.com

10/14/2005

Milestone 1: Target of Evaluation Description

- - - Begin Protection Profile Text - - -

Target of Evaluation Description

This Protection Profile specifies the minimum security requirements for a Target of Evaluation (TOE) that is a SCADA field device. Common functions of a SCADA field device include:

- Collecting measurements from sensors
- Making logic and control calculations
- Issuing control commands that modify a process

Examples of product categories that would be included in this TOE description are programmable logic controllers (PLC's), remote terminal units (RTU's), programmable automation controllers (PAC's), and intelligent electronic devices (IED's). These field devices are typically found in remote sites in SCADA networks such as pumping plants, substations, or turnouts.

The functionality of a field device can vary a great deal. Sophisticated field devices can run programs and control complex processes. Simple field devices can be limited to a small number of measurements and controls. This Protection Profile is applicable to any field device without regard to the amount of measurement, calculation or control that takes place in the device.

While the title of this Protection Profile refers to SCADA field devices, it may be applicable to similar field devices used in a DCS or any other control or monitoring system. In fact many field devices that are used in SCADA systems are also used in DCS and PLC based control systems.

The TOE includes all resident software, hardware, and firmware in a field device. The communication path and channels to the TOE are not part of the TOE. A simple way to describe the TOE boundary is the physical boundary around the hardware platform. The TOE boundary begins when data arrives at a physical interface and ends when data leaves a physical interface.

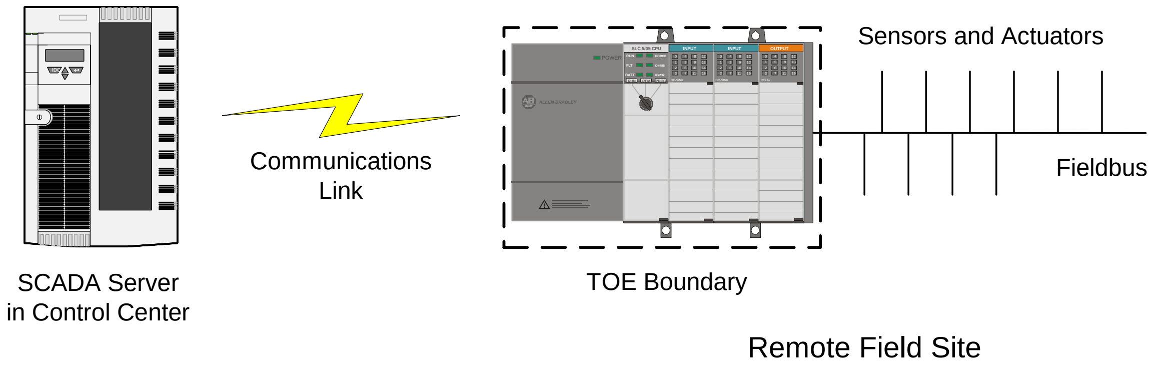

Figure 1 – TOE Boundary

Users are outside of the TOE boundary. They do however interact with the TOE through TOE Security Functions (TSF). Examples of this are user authentication for TOE management and access control requirements based on a user id or role.

Similarly, external IT entities are outside of the TOE boundary. A HMI or SCADA control server may communicate with the TOE, but these external IT entities and their communication links to the TOE are not in the TOE. The Protection Profile does have requirements to validate the integrity and reasonableness of external information when it arrives inside the TOE.

A TOE responding to this Protection Profile can either be a monolithic TOE or a component TOE that is part of a larger SCADA system or subsystem composite TOE.

- - - End Draft Protection Profile Text - - -

Explanatory Text

The TOE Description section is a simple and easily understood section in a Protection Profile. A TOE is the product or subsystem that would be tested for compliance with the Protection Profile. The process goes as follows:

1. A customer or industry group develops a Protection Profile with security functional and assurance requirements. The functional requirements define the what security is required in the TOE. The assurance requirements define how the vendor will need to prove the TOE meets the functional requirements. Protection Profiles are implementation independent, so two vendors could have different security approaches to meeting the functional requirements.
2. A vendor writes a Security Target document that responds to the Protection Profile with the implementation specific requirements for a TOE, a product.
3. The TOE is the product that is tested by a Common Criteria Testing Lab to prove it meets the requirements in a Security Target.

The TOE Description section in a Protection Profile describes the general functionality of products that could be a TOE and the boundaries of a TOE. In the SCADA Field Device Protection Profile this is very straightforward. A field device is typically a PLC, PAC, RTU, or IED. This is not a restrictive list of possible TOE’s, merely examples that contain the general functionality. Another class of field device, such as a smart instrument, could also use this Protection Profile.

The TOE boundary is the physical enclosure. All software, hardware and firmware in the physical box are within the TOE boundary. The communication links to the field device and the person or device that communicates with the field device are outside the boundary. This does not mean there will be no security requirements on data as it enters the TOE boundary; there will be.

Another piece of Common Criteria nomenclature in this section is the type of TOE. There are three types of TOE's:

1. Monolithic TOE – A self-contained, standalone TOE. This is a product or subsystem that does not have any component TOE's and is not part of a composite TOE.
2. Component TOE – The lowest level TOE in a system compromised of multiple TOE's. Two or more component TOE's can be combined to form a composite TOE.
3. Composite TOE – A composite of multiple component and composite TOE's that address requirements for a system.

A field device can be a monolithic TOE and can be evaluated and certified on its own. A field device can also be a component TOE that would be part of a composite TOE developed in the future. This composite TOE could include a Field Device Protection Profile and a Control Center Protection Profile.

Acronyms

DCS	Distributed Control System
IED	Intelligent Electronic Device
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller
PP	Protection Profile
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TOE	Target of Evaluation
TSF	TOE Security Functions

Next Milestone: Architectures, threats, vulnerabilities and risks for SCADA Field Devices

PLEASE SUBMIT COMMENTS FOR MILESTONE 1 BY OCTOBER 24, 2005

SUBMIT COMMENTS TO: peterson@digitalbond.com